REMARKS

This responds to the Final Office Action mailed on June 10, 2005. Reconsideration is respectfully required.

By this amendment, claims 1, 2, 4, 7 and 15 - 22 are amended, claim 14 is canceled, and no claims are added; as a result, claims 1 – 13 and 15 - 23 are now pending in this application.

RESPONSE TO EXAMINER STATEMENT

In the final office action dated 6/10/05 on page 11 under "Response to Arguments", the Examiner stated that "Regarding Applicant's argument that Downs fails to teach the use of a separate authentication code along with measurement parameters, this limitation is not in the claims and is therefore not considered."

Applicant respectfully submits that claims 14, 17 and 22 did recite the use of an authentication code that the authentication code is used to authenticate the measurement parameters. **Applicant respectfully requests that this limitation be considered by the Examiner and that a new office action be issued accordingly.**

§112 Rejection of the Claims

Claims 2, 3 and 10-13 were rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Claim 2 has been amended to delete the reference to "personal". In view of this, Applicant submits that the rejections of claims 2, 3 and 10 – 13 under 35 U.S.C. § 112 has been overcome.

§103 Rejection of the Claims

Claims 1, 4, 6-9 and 15 were rejected under 35 USC § 103(a) as being unpatentable over Wiser et al. (U.S. 6,385,596), further in view of Hardjono (U.S. 6,182,214) and further in view of Johnston (U.S. 6,373,946).

Claims 2, 3, 10-14 and 16-23 were also rejected under 35 USC § 103(a) as being unpatentable over Wiser et al., Hardjono, and Johnston, further in view of Downs et al. (U.S. 6,226,618) and further in view of Marvit et al. (U.S. 6,625,734).

Claim 5 was also rejected under 35 USC § 103(a) as being unpatentable over Wiser et al., Hardjono, and Johnston, and further in view of Howard et al. (U.S. 2002/0069365).

Applicant's claim 1, as amended, is directed to controlling content usage in a wireless communication device. The wireless communication device has two or more processors and a decryption key is divided into at least first, second and third key-shares to control usage of the content. As recited in claim 1, for example, the third key-share is pre-stored in the wireless communication device. The wireless communication device is provided the first key-share in response to a request for content and the wireless communication device is provided the second key-share when credit of a user of the wireless communication device is verified. Upon receipt of the content, a security processor of the wireless communication device combines the first and second key-shares with the third key-share for use in decrypting the content. The security processor also monitors usage of the content and purges at least one of the key shares when usage of the content exceeds one or more measurement parameters. The security processor also authenticates the measurement parameters using an authentication code to help prevent tampering with the measurement parameters. A communication processor plays the decrypted content. The measurement parameters are secured by the authentication code and provided by a security server over the wireless link along with encrypted content. Claims 16 and 21 are similar.

Applicant submits that none of the cited references disclose (among other things) a multi-processor device having a communication processor and a security processor, and the use of an authentication code to authenticate and help prevent tampering with measurement parameters. The cited references primarily are directed to secure distribution of content and are not concerned with usage of content once the content is at the user device. This is discussed in more detail below.

Discussion of Wiser

Wiser is cited by the Examiner for controlling content usage in a communication device. Applicant submits, however, that Wiser is not directed to controlling content *usage*, but is directed to controlling content *distribution* using a decryption key and other information (see Wiser, columns 3 line 5 through column 5 line 15). Applicant finds nothing in Wiser to control content usage on a wireless communication device particular by monitoring content usage against measurement parameters. In Wiser, it appears that once a user has the content, the user is free to use it in any way he or she pleases.

Wiser uses a single private decryption key that is provided to the user which results in a security risk. Therefore Wiser must secure the private key with a strong symmetric key when transferring the private key to the user (see Wiser column 4, lines 24 – 27). Applicant's claims solve this problem with the use of key shares. Applicant further submits that there would be no reason for Wiser to use key shares because Wiser uses a digital passport and/or certificate to authenticate the purchaser to the content manager and deliver server (see Wiser column 4, lines 13 – 31). This teaches away from the use of key-shares that are stored and/or provided by the various elements of Applicant's system to allow a user to decrypt and play content. In view of this, Applicant submits that there would be no reason or motivation to combine Wiser with Hardino (which divides a secret into shares).

Discussion of Downs

Downs is cited for teaching usage conditions. Applicant's claims 1, 16 and 21 recite monitoring usage of content with measurement parameters. Applicant submits that Downs does not teach monitoring content usage with measurement parameters. Downs only discloses 'usage conditions' (see Downs column 9). These usage conditions are different than the measurement parameters of Applicant's claims which are used to *measure how* decrypted content is actually used in a wireless device. *There are no teachings in Downs to monitor or measure how content is actually used* (e.g., the number of times media can be played, a time-frame the content can be used for, etc.). In Downs, the usage conditions are simply Metadata entered for particular content (see Downs, column 9, lines 32 – 36) and are limited to copy restriction, wholesale price and business rules. There is no mention in Downs how these usage conditions are used, and in

particular, there is no mention that actual use of content is actually *monitored* against these usage conditions. Furthermore, these usage conditions in Downs are not secured in any way separate from the content itself. Metadata can easily be modified by a user.

In Applicant's claims 1, 16 and 21, the measurement parameters are secured with an authentication code provided by the content provider. The measurement parameters are authenticated using the authentication code to determine if they have been tampered with. If the security processor determines that the measurement parameters have been tampered with (e.g., failure to authenticate), one of the key shares can be purged from the wireless communication device to prevent further usage of the content. See, for example, claims 2, 17 and/or 22 which recite that a key share is purged when either the usage of the content exceeds service limit indicated by the measurement parameters or when the authentication code fails to authenticate. Applicants find no such teachings in Downs.

Discussion of Marvit

Marvit has been cited by the Examiner for purging a key. Applicant's claims 1, 16 and 21, however, do not recite purging a key, but recite purging only a portion of a key (i.e., purging a key share). Applicant's claims 1, 16 and 21 further recite that the key share is purged from the wireless communication device, not a key repository. Applicant purges the key share from the wireless device when usage of content exceeds one of the measurement parameters. Applicant's claims 2, 17 and 22 further recite purging a key share when either the usage of the content exceeds service limit indicated by the measurement parameters or when the authentication code fails to authenticate. Marvit, however, deletes a key from the key repository to make the message become unusable. Marvit, however, does not delete the key within the user device because Marvit doesn't care about use of the message by the user. Once the user decrypts and reads the message, there is no reason to further secure the message at the user device. Marvit's purpose is to secure a message (e.g., an email) while it is temporarily stored at various locations in transit within the Internet (see Marvit column 1, lines 27 – 40), and to provide a way to delete the message from all these temporary storage locations (see Marvit column 1 lines 40 - 49).

Applicant's claims on the other hand, do not delete an entire key, and do not delete the key at a key repository to making the content unusable at a key repository. Applicant is concerned with the use of the content on a particular wireless communication device.

Discussion of Johnston

Johnston has been cited by the Examiner for disclosing a wireless communication device. Applicant's claims 1, 16 and 21 recite a multi-processor wireless communication device having both a security processor and a communication processor. Applicant finds no such teachings in Johnston. In Johnston, a key is stored on a SIM (see Johnston abstract). Applicant's claim 21, for example, recites that a first key-share is pre-stored in the processor area and the second-key-share is pre-stored in the SIM prior to the device generating the request for the content and prior to a security server sending the content and the third-key-share to the wireless communication device. These recitations are not taught by Johnston.

Discussion of Hardino

Hardino has been cited by the Examiner for the use of key shares and the pre-storing of one on a device. Applicant respectfully disagrees with the Examiner and submits that Hardino does not teach, suggest or motivate the storing of a key-share on a user device. Hardino only states that a number of entities having at least M shares between them can cooperate to reconstruct a secret (see column 3, lines 33 – 42).

In summary, Applicant submits that the combination of Wiser, Hardino, Johnston, Downs and Marvit, does not result in Applicant's invention as recited in claims 1, 16 and 21. None of the references separately teach, suggest or provide motivation for at least the following:

1) a wireless communication device having two processors;

2) a security processor to combine key-shares, decrypt content, monitor usage of the content against measurement parameters, and to authenticate the measurement parameters with an authentication code;

3) a separate communication processor to play the decrypted content; and

4) using an authentication code to help prevent tampering with the measurement parameters.

None of the references further separately teach, suggest or provide motivation for purging at least one of the key-shares when usage of the content exceeds a service limit indicated by the measurement parameters, or when the authentication code fails to authenticate, as recited in claims 2, 17 and 22.

Applicant submits that since none of these elements are disclosed by any of Wiser, Hardino, Johnston, Downs and Marvit, the combination of Wiser, Hardino, Johnston, Downs and Marvit cannot result in Applicant's claimed invention.

Claims 11 and 19, for example, further recite that the measuring parameters comprise at least one of a date-limit, a run-time limit, and an iteration limit.

Claim 12 further recites that the content server defines the set of measurement parameters based on preferences of a content provider.

Claim 13 further recites that the date-limit defines an end calendar date for playing the content, the run-time limit defines a maximum amount of time for playing portions of the content, and the iteration limit defines a maximum number of times for playing the content or portions thereof.

Claim 20 further recites that the processing system has, in addition to the security processor and the communications process, an applications processor to process applications running on the wireless communication device. Claim 20 further recites that the security processor portion, communications processor portion and applications processor portion are part of a processor area and fabricated on an application specific integrated circuit (ASIC).

None of these recitations are disclosed by Wiser, Hardino, Johnston, Downs and Marvit, either separately or in combination.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applciant's attorney, Greg Gorrie at (480) 659-3314, or Applciant's below-named representative to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

ERNEST E. WOODWARD

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Attorneys for Intel Corporation
P.O. Box 2938
Minneapolis, Minnesota 55402
(612) 349-9592

Date Aug. 10, 2005 By Ann M. McCrackin

Ann M. McCrackin
Reg. No. 42,858

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 10th day of August 2005.

John M. Gustav-Wrathall

Name

Signature